FACTORIZATIONS OF FINITE GROUPS BY CONJUGATE SUBGROUPS WHICH ARE SOLVABLE OR NILPOTENT

MARTINO GARONZI, DAN LEVY, ATTILA MARÓTI, AND IULIAN I. SIMION

Abstract. We consider factorizations of a finite group G into conjugate subgroups, $G = A^{x_1} \cdots A^{x_k}$ for $A \leq G$ and $x_1, \ldots, x_k \in G$, where A is nilpotent or solvable. First we exploit the split BN-pair structure of finite simple groups of Lie type to give a unified self-contained proof that every such group is a product of four or three unipotent Sylow subgroups. Then we derive an upper bound on the minimal length of a solvable conjugate factorization of a general finite group. Finally, using conjugate factorizations of a general finite solvable group by any of its Carter subgroups, we obtain an upper bound on the minimal length of a nilpotent conjugate factorization of a general finite group.

1. Introduction

In this paper we continue the study of minimal length factorizations of (mainly finite) groups into products of conjugate subgroups, that was initiated in [17] and [8]. For a group G and $A \leq G$, a conjugate product factorization (a cp-factorization) of length k of G by A, is a factorization $G = A_1 \cdots A_k$ where $A_1, \ldots, A_k$ are all conjugate to A and the product is the setwise product. Denoting the normal closure of A in G by A^G, an elementary argument shows that A^G is equal to a product of conjugates of A (see [22]). Thus, a necessary condition (and for finite groups also a sufficient condition) for the existence of the factorizations we are interested in, is $G = A^G$.

Definition 1.1. *Let G be a group and $A \leq G$. Then $\gamma_{\mathrm{cp}}^{A}(G)$ is the smallest number k such that G equals a product $A_1 \cdots A_k$ of conjugates of A or ∞ if no such k exists. We also set*

$$\gamma_{\mathrm{cp}}(G) := \min\{\gamma_{\mathrm{cp}}^{A}(G) | A < G\},$$

where $\min\{\infty\} := \infty$.

It is easy to see that $\gamma_{\mathrm{cp}}^{A}(G) \geq 3$ if $A < G$ ([17, Lemma 6]). For finite, non-nilpotent, solvable groups $\gamma_{\mathrm{cp}}(G) \leq 4 \log_2 |G|$ [1] and no universal constant upper bound exists for all G (see [17, Theorems 4 and 5]). In contrast, if G is a finite non-solvable group, then $\gamma_{\mathrm{cp}}(G) = 3$ ([8]). Moreover, in [8] we proved that $\gamma_{\mathrm{cp}}(G) = 3$

Date: March 9, 2015.

2000 *Mathematics Subject Classification.* 20B15, 20B40, 20D05, 20D20, 20D40, 20E42 .

Key words and phrases. products of conjugate subgroups, Sylow subgroups.

M.G. acknowledges the support of MIUR-Italy via PRIN Group theory and applications.

A.M. acknowledges the support of an Alexander von Humboldt Fellowship for Experienced Researchers and the support of OTKA K84233.

I.S. acknowledges the support of the University of Padova (grants CPDR131579/13 and CPDA125818/12).

[1] In fact, this bound is somewhat improved by Theorem 1.4 below.

holds for any group G with a BN-pair and a finite Weyl group, and this optimal result arises from choosing A to be the Borel subgroup of G which is in particular solvable. This motivated us to diversify the analysis of cp-factorizations in the present paper by imposing conditions on the subgroup A.

Let G be a finite simple group of Lie type whose defining characteristic is p. The first problem we consider is the cp-factorization of G by Sylow p-subgroups (also called unipotent Sylows). Liebeck and Pyber have proved ([25, Theorem D]) that G is a product of no more than 25 Sylow p-subgroups. Several papers considering the same question then followed. In [3] it was claimed that the 25 can be replaced by 5, however a complete proof has not been published. A sketch of a proof of this claim for exceptional Lie type groups appears in a survey by Pyber and Szabó ([27, Theorem 15]). Smolensky, Sury and Vavilov ([34, Theorem 1]) consider the problem of unitriangular factorizations of Chevalley groups over commutative rings of stable rank 1. When specializing their results to elementary Chevalley groups over finite fields, they get that any non-twisted finite simple group of Lie type is a product of four unipotent Sylows. Later on, these results were extended by Smolensky in [29] to cover some twisted Chevalley groups over finite fields or the field of complex numbers.

In Section 2 we give a unified self-contained treatment of the problem of finding minimal length products of unipotent Sylows for all finite simple groups of Lie type, exploiting their split BN-pair structure. Recall that a Carter subgroup of a finite group G is a self-normalizing nilpotent subgroup (see [9]).

Theorem 1.2. *Let G be a simple group of Lie type whose defining characteristic is p. Let U be a Sylow p-subgroup of G and set $U^- := U^{n_o}$, where n_0 is a representative of the longest element of the associated Weyl group. Then $G = (UU^-)^2$, and $G = UU^-U$ if and only if U is a Carter subgroup. In both cases these factorizations are of minimal length.*

After the completion of our proof of Theorem 1.2, and in parallel to its publication in preprint form ([18]), Smolensky made available a preprint in which he shows that every Suzuki and Ree group is a product of four unipotent Sylow subgroups ([30]). Thus, the results in [32],[33],[34],[29] and [30], combine to give a different proof of the four Sylow claim of Theorem 1.2.

Theorem 1.2 and the cp-factorization of finite simple groups of Lie type by Borel subgroups mentioned above clearly motivate a general study of cp-factorizations of a finite group G by subgroups which are nilpotent or solvable. Observe that if G is any finite group then it is equal to the product of a finite number of conjugates of a nilpotent (hence also solvable) $A \leq G$. For if G is nilpotent or $A < G$ is both nilpotent and non-normal maximal, the claim is clear. Otherwise $G = A_1 \cdots A_k$ is a cp-factorization where A_1 is some maximal non-normal subgroup of G, and by induction A_1 has a nilpotent cp-factorization. Therefore, for a finite group G the following quantities are always natural numbers:

$$\gamma^{\mathrm{s}}_{\mathrm{cp}}(G) := \min\{\gamma^{A}_{\mathrm{cp}}(G) | A \leq G \text{ is solvable}\}.$$

$$\gamma^{\mathrm{n}}_{\mathrm{cp}}(G) := \min\{\gamma^{A}_{\mathrm{cp}}(G) | A \leq G \text{ is nilpotent}\}.$$

Note that $\gamma^{\mathrm{s}}_{\mathrm{cp}}(G) = 1$ ($\gamma^{\mathrm{n}}_{\mathrm{cp}}(G) = 1$) if and only if G is solvable (nilpotent). In Section 3 we prove the following upper bound on $\gamma^{\mathrm{s}}_{\mathrm{cp}}(G)$ in terms of the quantity $|G|_{\mathrm{nab}}$, defined as the product of the orders of all non-abelian composition factors of G (if G is solvable, $|G|_{\mathrm{nab}} := 2$).

Theorem 1.3. *For any finite group G, we have $\gamma_{\mathrm{cp}}^{\mathrm{s}}(G) \leq 1 + c_S(\log_2 \log_2 |G|_{\mathrm{nab}})^2$, where $0 < c_S \leq 12/\log_2(5) < 5.17$ is a universal constant.*

Using Theorem 1.3 we can reduce the problem of obtaining an upper bound on $\gamma_{\mathrm{cp}}^{\mathrm{n}}(G)$ for a general finite group G to a solvable G. Moreover, it turns out that there is a judicious choice of a nilpotent subgroup in the case that G is solvable - that of a Carter subgroup (see above and Lemma 4.3). The following theorem is proved in Section 4.

Theorem 1.4. *Any finite solvable group G is a product of at most $1+c_A \log_2 |G : C|$ conjugates of a Carter subgroup C, where $0 < c_A \leq 3/\log_2(5) < 1.3$ is a universal constant.*

Corollary 1.5. *For any finite group G there exists a nilpotent $H \leq G$ such that*

$$\gamma_{\mathrm{cp}}^{\mathrm{n}}(G) \leq \gamma_{\mathrm{cp}}^{H}(G) \leq 1 + c_S c_A \left(\log_2 |G : H|\right) \left(\log_2 \log_2 |G|\right)^2 .$$

The proof of Theorem 1.4 requires the following result which is of independent interest.

Theorem 1.6. *Let G be a finite affine primitive permutation group with a non-trivial point stabilizer H. Then G is a product of at most $1 + c_A \log_2 |G : H|$ conjugates of H, where $0 < c_A \leq 3/\log_2(5) < 1.3$ is a universal constant.*

A natural question to ask, in view of the last theorem, is to what extent can it be generalized to an arbitrary finite primitive permutation group. We plan to consider this question separately ([19]).

2. Factorizations by unipotent Sylow subgroups

The proof of Theorem 1.2 consists of two main steps: 1. A reduction to the case of a two element Weyl group (i.e., $W = Z_2$, and we shall say that G is a "rank 1 group"), which is carried within the framework of groups with a split BN-pair, and some extra assumptions to be detailed in the sequel. 2. A derivation of a general necessary and sufficient criterion for rank 1 groups satisfying an extended set of split BN-pair assumptions, that is then verified to hold for the special case of groups with a σ-setup, using a result from [12].

We would like to point out that although the proof of [34, Theorem 1] also uses a "reduction to rank 1 argument" which is due to Tavgen′ ([32]), we do not know if there is a more direct relation between this approach and ours.

We treat simple groups of Lie type in the setting of groups with a σ-setup as in [20, Definition 2.2.1]. For this fix a prime p, a simple algebraic group $\overline{K}$ defined over $\overline{\mathbb{F}}_p$ and a Steinberg endomorphism σ of $\overline{K}$, and consider K - the subgroup of $C_{\overline{K}}(\sigma)$ generated by all p-elements. All groups K obtained in this way are said to have a σ-setup given by the pair $(\overline{K}, \sigma)$. The set of all groups possessing a σ-setup for the prime p is denoted by $\mathcal{L}ie(p)$. We have surjective homomorphisms $K_u \longrightarrow K \longrightarrow K_a$ with central kernels ([20, Theorem 2.2.6]), where the groups $K_u, K_a \in \mathcal{L}ie(p)$ are called the universal and the adjoint version of K, respectively. Due to the classification of simple groups of Lie type, if we exclude the Tits group ${}^2F_4(2)'$, then all such groups lie in $\mathcal{L}ie(p)$ for some p appearing as the adjoint version K_a of some K. Set $\mathcal{L}ie := \cup \mathcal{L}ie(p)$ the union over all primes p. For $G \in \mathcal{L}ie$ we have (see [10, Chapter 2]):

(i) G is a group with a split BN-pair (B,N) and a finite Weyl group W, where $B = H \ltimes U$,
(ii) U is a Sylow p-subgroup of G,
(iii) G is generated by its p-elements.

2.1. **Reduction to $|W| = 2$ case for groups with a split BN-pair.** For our purposes we will call a triple (H,U,N) a split BN-pair for a group G if $(H \ltimes U, N)$ satisfies the axioms of split BN-pairs in [10, §2.5] with respect to H and U. We assume that the Weyl group $W = N/H$ of the BN-pair is finite (this certainly holds for finite groups), and so the longest element $w_0 = n_0 H$ of W exists and defines subgroups $U^- := U^{n_o}$ and $B^- := B^{n_o}$. For $w \in W$ we sometimes use $\dot{w}$ to denote an arbitrary choice of an element of N such that $w = \dot{w}H$. We use the notation U^-, X_i, U_i, X_{-i}, U_w from [10, §2.5] for the BN-pair (B,N) and we label with the upper-script '$-$' the corresponding subgroups for (B^-,N), i.e. when U and B are replaced by U^- and B^- everywhere: $(U^-)^-$, X_i^-, U_i^-, X_{-i}^-, U_w^-. Note that $(U^-)^- = U$, $X_i^- = X_{-i}$, $X_{-i}^- = X_i$ and that $X_i = U_s$ and $X_{-i} = U_s^-$ for some simple reflection s. In addition, define $L_s := \langle U_s, U_s^-, H\rangle$ and $G_s := \langle U_s, U_s^-\rangle$ for any simple reflection $sH \in W$. Furthermore, we assume that the root subgroups X_α, $\alpha \in \Phi$ (Φ is the set of roots associated with W) satisfy the commutator relations ([10, p.61]).

Lemma 2.1. *Let G be a group with a split BN-pair (H,U,N). Suppose that G is a product of k conjugates of U ($k \geq 3$ an integer). Then*

$$G = UU^-UU^- \cdots UU^-U^\varepsilon,$$

where $\varepsilon \in \{+,-\}$, $U^+ = U$, the total number of non-trivial conjugates of U which appear on the r.h.s. is k, and $\varepsilon = +$ if and only if k is odd.

Proof. We have $\gamma_{\mathrm{cp}}^U(G) = k \Leftrightarrow G = U^{x_1}U^{x_2}\cdots U^{x_k}$ for some elements $x_1,\ldots,x_k \in G$. This is equivalent to $G = Ug_1U\cdots Ug_{k-1}U$ for some $g_1,\ldots,g_{k-1} \in G$ (see [8, §2 Lemma 1]). By the Bruhat expression of elements (w.r.t. H and U) we may assume that $g_i \in N$ for all i. Indeed, by [10, Theorem 2.5.14], for each $1 \leq i \leq k-1$, we have $g_i = u_i h_i \dot{w}_i u_i'$ where $u_i \in U$, $h_i \in H$, $w_i \in W$ and $u_i' \in U_w \leq U$. Since the h_i lie in $N_G(U)$ we have $Ug_1U\ldots Ug_{k-1}U = Uh_1\dot{w}_1U\ldots Uh_{k-1}\dot{w}_{k-1}U = U\dot{w}_1U\ldots U\dot{w}_{k-1}U(h_1^{\dot{w}_1\cdots\dot{w}_{k-1}}\cdots h_{k-1})$ so $\gamma_{\mathrm{cp}}^U(G) = k$ is equivalent to $G = Ug_1U\ldots Ug_{k-1}U$ for some $g_1,\ldots,g_{k-1} \in N$. This is equivalent to $G = UU^{g_1^{-1}}U^{g_2^{-1}}\cdots U^{g_{k-1}^{-1}}$ for some $g_1,\ldots,g_{k-1} \in N$ (see proof of [8, §2 Lemma 1]).

Let $n \in N$ be arbitrary, and let $w = nH$. By [10, Proposition 2.5.12] we have

$$U = U_{w_0w}U_w = \left(U \cap U^{n_0(n_0n)}\right)\left(U \cap U^{n_0n}\right),$$

which gives

$$U^{n^{-1}} = \left(U \cap U^{n_0(n_0n)}\right)^{n^{-1}}\left(U \cap U^{n_0n}\right)^{n^{-1}} = \left(U^{n^{-1}} \cap U\right)\left(U^{n^{-1}} \cap U^{n_0}\right) \leq UU^-.$$

However, since U, U_{w_0w}, U_w are all subgroups, $U = U_{w_0w}U_w$ implies $U = U_wU_{w_0w}$, and hence we also get $U^{n^{-1}} \leq U^-U$. Therefore:

$$G = UU^{g_1^{-1}}U^{g_2^{-1}}\cdots U^{g_{k-1}^{-1}} \subseteq U\left(UU^-\right)\left(U^-U\right)\left(UU^-\right)\left(U^-U\right)\cdots = UU^-UU^-U\cdots,$$

where we have used $U^2 = U$ and $\left(U^-\right)^2 = U^-$, and the claim follows. □

In the following lemma we collect known results about minimal (non-abelian) Levi subgroups which will be used in the sequel. First note that for a fixed split BN-pair (H, U, N) we have *the (split) BN-pair opposite to* (B, N) given by (H, U^-, N). Clearly, for any $g \in G$, (B^g, N^g) is a split BN-pair, and if $g \in N$ then $B^g \cap N = H$ so $B^g = H \ltimes U^g$. In particular this applies to $g = n_0$.

Lemma 2.2. *Let G have a split BN-pair (H, U, N). Let w_0 be the longest element of the Weyl group N/H and $s = n_s H$ a simple reflection with respect to (H, U, N). Then*

(a) $U = U_s U_{w_0 s} = U_{w_0 s} U_s$ *and* $U^- = U_s^- U_{w_0 s}^- = U_{w_0 s}^- U_s^-$,
(b) $L_s \subseteq N_G(U_{w_0 s}) \cap N_G(U_{w_0 s}^-)$.

Proof. Any $s = n_s H$ in W is simple with respect to (H, U, N) if and only if it is simple with respect to (H, U^-, N): This follows from [10, Propositions 2.2.6 and 2.2.7] and the fact that the positive roots with respect to (H, U^-, N) are the negative roots with respect to (H, U, N). So $I := \{s_1, ..., s_l\}$, the set of simple reflections for (H, U, N), is a set of simple reflections for both of these BN pairs and $s = s_i$ for some $i \in \{1, \dots, l\}$. Since L_s is the subgroup $X_i H \cup X_i H n_i X_i = \langle X_i, X_{-i}, H\rangle$ (see [10, Corollary 2.6.2]), $X_i^- = X_{-i}$ and $X_{-i}^- = X_i$, it follows that $L_s = \langle X_i^-, X_{-i}^-, H\rangle$ is a (minimal) standard Levi subgroup with respect to both (B, N) and (B^-, N).

Now (a) follows from [10, Proposition 2.5.11] and (b) is a particular case of [10, Proposition 2.6.4]. □

The following lemma is [34, Lemma 4].

Lemma 2.3. *Let G be a group and let $X \subseteq G$ satisfy $X = X^{-1}$ and $G = \langle X\rangle$. If $\emptyset \neq Y \subseteq G$ is such that $XY \subseteq Y$ then $Y = G$.*

Proposition 2.4. *Let G be a group with a split BN-pair such that the conjugates of U in G generate G. Let $k \geq 2$ be an integer and assume further that $G_s = (U_s U_s^-)^k$ for every simple reflection s then $G = (UU^-)^k$.*

Proof. Set $X := \{u^g | u \in U, g \in G\}$. Then $X = X^{-1}$ since U is a subgroup of G, and $G = \langle X\rangle$ since G is the normal closure of U. Set $Y := (UU^-)^k$. By Lemma 2.3 our claim will follow if we show that $XY \subseteq Y$. Thus it suffices to show that $u^g Y \subseteq Y$ for any $u \in U$ and $g \in G$. By [10, Theorem 2.5.14], for any $g \in G$ there exist $u' \in U$, $h \in H$, $w \in W$ and $u'' \in U_w \leq U$ such that $g = u' h n_w u''$. Hence $u^g = u^{u' h n_w u''} = \left(u^{u' h}\right)^{n_w u''}$. But $u^{u' h} \in U$, so it is sufficient to prove that $u^{nv} Y \subseteq Y$ for all $u, v \in U$ and $n \in N$. Now we claim that the last statement follows if we prove that N normalizes Y. For suppose that N normalizes $Y = (UU^-)^k$. We have:

$$
\begin{aligned}
u^{nv}\left(UU^-\right)^k &= v^{-1}n^{-1}unv\left(UU^-\right)^k = v^{-1}n^{-1}un\left(UU^-\right)^k = \\
&= v^{-1}n^{-1}u\left(UU^-\right)^k n = v^{-1}n^{-1}\left(UU^-\right)^k n = \\
&= v^{-1}\left(UU^-\right)^k n^{-1}n = \left(UU^-\right)^k .
\end{aligned}
$$

Thus we prove that N normalizes $(UU^-)^k$. Since H clearly normalizes $(UU^-)^k$, and N is generated by a set I of representatives for simple reflections together with H, it is sufficient to prove that $(UU^-)^k$ is normalized by all n in I. Fix a simple

reflection $s = nH$. By Lemma 2.2.(a), $UU^- = U_s U_{w_0 s} U^-_{w_0 s} U^-_s$. By Lemma 2.2.(b), each of U_s and U^-_s commutes with both $U_{w_0 s}$ and $U^-_{w_0 s}$. This, and the assumption $G_s = (U_s U^-_s)^k$, give:

$$\left(UU^-\right)^k = \left(U_s U^-_s\right)^k \left(U_{w_0 s} U^-_{w_0 s}\right)^k = G_s \left(U_{w_0 s} U^-_{w_0 s}\right)^k.$$

Since $L_s = G_s H$ we can assume $n \in G_s$ and hence $nG_s = G_s n$. Since $n \in G_s \leq L_s$, Lemma 2.2.(b) gives $n\left(U_{w_0 s} U^-_{w_0 s}\right)^k = \left(U_{w_0 s} U^-_{w_0 s}\right)^k n$. Combining everything together yields:

$$\begin{aligned} n\left(UU^-\right)^k &= nG_s \left(U_{w_0 s} U^-_{w_0 s}\right)^k = G_s n \left(U_{w_0 s} U^-_{w_0 s}\right)^k = \\ &= G_s \left(U_{w_0 s} U^-_{w_0 s}\right)^k n = \left(UU^-\right)^k n, \end{aligned}$$

and the proof that N normalizes $\left(UU^-\right)^k$ is concluded. □

Remark 2.5. *If G is generated by U and U^- then, in the above proof, Lemma 2.3 can be avoided: if N normalizes $\left(UU^-\right)^k$ then $\left(UU^-\right)^k$ is stable in particular under conjugation by $n_0 H$ so it equals $\left(U^- U\right)^k$. It is easy to see that if this equality holds then $G = (UU^-)^k$.*

2.2. **The case $|W| = 2$.**

Lemma 2.6. *Let G be a group with a split BN-pair (H, U, N) and a Weyl group $W = \{1, s_1\}$. Set $\left(U^-\right)^* := U^- - \{1\}$. Fix an arbitrary $n_1 \in N$ such that $s_1 = n_1 H$, and set*

$$\widetilde{H} := \left\{ h \in H | \exists u^- \in \left(U^-\right)^*,\ Uu^- U = Un_1 hU \right\}.$$

Then:

(a) $U\left(U^-\right)^* U = Un_1 \widetilde{H} U$.

(b) $UU^- UU^- = UU^- \left(\{1\} \cup n_1 \widetilde{H} n_1 \widetilde{H}\right) \cup Un_1 \widetilde{H}$.

Proof. (a) Since $W = \{1, s_1\}$ we have

$$G = B \cup Bn_1 B = UH \cup UHn_1 HU = UH \cup Un_1 HU,$$

where the union on the right is disjoint. By [10, Proposition 2.5.5(i)], $B \cap U^- = 1$. Hence $\left(U^-\right)^* \subseteq Un_1 HU$. Thus, for every $u^- \in \left(U^-\right)^*$ there exist $h \in H$ such that $Uu^- U = Un_1 hU$. But, by definition, $h \in \widetilde{H}$, so this proves $U\left(U^-\right)^* U \subseteq Un_1 \widetilde{H} U$. The reverse inclusion is also clear and hence $U\left(U^-\right)^* U = Un_1 \widetilde{H} U$.

(b) Note that since each element of H normalizes both U and U^-, the set $\widetilde{H}$ commutes with U. Also, $w_0 = s_1$ and hence $n_1 U n_1^{-1} = U^-$ and $n_1 U^- n_1^{-1} = U$. Given this and the relation in (a) we get:

$$\begin{gathered} UU^- UU^- = U\left(U^-\right)^* UU^- \cup UU^- = Un_1 \widetilde{H} UU^- \cup UU^- = \\ = UU^- n_1 \widetilde{H} U^- \cup UU^- = UU^- U n_1 \widetilde{H} \cup UU^- = \\ = U\left(U^-\right)^* Un_1 \widetilde{H} \cup Un_1 \widetilde{H} \cup UU^- = \\ = Un_1 \widetilde{H} Un_1 \widetilde{H} \cup Un_1 \widetilde{H} \cup UU^- = UU^- n_1 \widetilde{H} n_1 \widetilde{H} \cup Un_1 \widetilde{H} \cup UU^- = \\ = UU^- \left(\{1\} \cup n_1 \widetilde{H} n_1 \widetilde{H}\right) \cup Un_1 \widetilde{H}. \end{gathered}$$ □

Lemma 2.7. *Let G be a group with a split BN-pair (H, U, N) and Weyl group $W = \{1, s_1\}$. Using the notation of Lemma 2.6, the following conditions are equivalent:*

(a) $(U^-)^* \cap Un_1hU \neq \emptyset$ *for all* $h \in H$. *Equivalently* $H = \widetilde{H}$.
(b) $U(U^-)^* U = Un_1HU$.
(c) $G = (UU^-)^2$.

Proof. By definition $\widetilde{H} \subseteq H$ and by Lemma 2.6 (a), $U(U^-)^* U = Un_1\widetilde{H}U$. Hence (a) and (b) are equivalent. To finish the proof observe that

$$G = B \cup Bn_1B = (B \cup Bn_1B)\, n_1 = Bn_1 \cup Bn_1Bn_1 = Bn_1 \cup BB^- = \\ = Un_1H \cup UU^-H,$$

where the union on the r.h.s. is disjoint. Since the sets $\widetilde{H}$ and $n_1\widetilde{H}n_1$ are both contained in H, we have $Un_1\widetilde{H} \subseteq Un_1H$, and $UU^-\left(\{1\} \cup n_1\widetilde{H}n_1\widetilde{H}\right) \subseteq UU^-H$. Since $G = Un_1H \cup UU^-H$ is a disjoint union, Lemma 2.6 (b) implies that $G = (UU^-)^2$ if and only if $Un_1\widetilde{H} = Un_1H$ and $UU^-\left(\{1\} \cup n_1\widetilde{H}n_1\widetilde{H}\right) = UU^-H$. Thus, by Lemma 2.6 (a), we get that (c) implies (b), and it is also clear that (a) implies (c). □

2.3. **Groups with a σ-setup.** Any $K \in \mathcal{L}ie$ has a split BN-pair (H, U, N), where U is a Sylow p-subgroup for the defining characteristic p, descending from the algebraic group $\overline{K}$ (see [20, Theorem 2.3.4]). More precisely, if $\overline{T} \subseteq \overline{B}$ is a pair of σ-stable maximal torus and Borel subgroup of $\overline{K}$ then $B = \overline{B} \cap K$ and $N = N_{\overline{K}}(\overline{T}) \cap K$ form a BN-pair for K and if $\overline{U}$ is the unipotent radical of $\overline{K}$, i.e., $\overline{B} = \overline{T} \ltimes \overline{U}$, then $B = H \ltimes U$ where $H = \overline{T} \cap K$ and $U = \overline{U} \cap K$ is a Sylow p-subgroup of K (as in [20, Section 3.4]).

Remark 2.8. *1.) Some groups in $\mathcal{L}ie$ have split BN-pairs for different primes p, e.g. $A_1(4) = A_1(5)$ (see* [20, Theorem 2.2.10]*).*

2.) If $K \in \mathcal{L}ie(p)$ then $K_s \in \mathcal{L}ie(p)$. Moreover if K is universal then so is K_s by [20, Theorem 2.6.5.(f)].

3.) Note also that if $\overline{K}$ is universal (see [20, Theorem 1.10.4]*) then, by a result of Steinberg (see* [26, Theorem 24.15]*), $K_u = C_{\overline{K}}(\sigma)$ so B, N, H and U are the centralizers of σ in $\overline{B}$, $\overline{N}$, $\overline{T}$ and $\overline{U}$ respectively.*

Lemma 2.9. *Let $K_u \in \mathcal{L}ie(p)$ be universal of rank 1 and let U be a Sylow p-subgroup of K_u. Then $K_u = (UU^-)^2$.*

Proof. First note that since K_u is universal, the corresponding algebraic group $\overline{K}_u$ is universal (or simply connected in a different terminology [20, Definition 1.10.5]). By Remark 2.8.3, K_u is a finite group of Lie type. The possible types for rank 1 are A_1, ${}^2A_2$, ${}^2B_2$ and ${}^2G_2$ (see for example [26, Table 23.1]) and the possibilities for $\overline{K}_u$ can be read off from [20, Theorem 1.10.7].

Let p be the defining characteristic of K_u. By [10, §1.19], we need to consider, for all powers q of p, the groups $\mathrm{SL}_2(q)$, $\mathrm{SU}_3(q^2)$, ${}^2B_2(q^2)$ if $p = 2$ and $q^2 = 2^{2n-1}$ for some $n \geq 0$ and ${}^2G_2(q^2)$ if $p = 3$ and $q^2 = 3^{2n-1}$ for some $n \geq 0$.

Now K_u satisfies the assumptions of Lemma 2.7, so, in particular we use the notation of Lemma 2.7. For $K_u = \mathrm{SL}_2(q)$ condition (a) of the lemma is easily verified - for the calculation see [11, §6.1]. For the remaining cases we use [12, Proposition 4.1]. By this result, for every $h \in H$ there exists $y \in U$ such that $yn_1 \in U^-hU = n_1^{-1}Un_1hU$. Multiplying by n_1^{-1} on the left, and using $\left(n_1^{-1}\right)^2 \in H$, we obtain $n_1^{-1}yn_1 \in Un_1\left(\left(n_1^{-1}\right)^2 h\right)U$. Observe that $1 \notin Un_1\left(\left(n_1^{-1}\right)^2 h\right)U$, and

hence $n_1^{-1}yn_1 \in (U^-)^*$. Moreover, as h varies over H, so does $\left(n_1^{-1}\right)^2 h$. Hence, condition (a) of Lemma 2.7 holds for this case, and the claim follows. $\square$

Remark 2.10. *Note that the groups denoted by* $\mathrm{SU}_n(q^2)$ *in* [10, §1.19] *are denoted by* $\mathrm{SU}_n(q)$ *in* [26, Example 21.2]. *Note also that for the groups* ${}^2B_2(2^{2n-1})$ *the universal and the adjoint versions are isomorphic (see* [10, §1.19]*). Moreover since the center* $Z(K_u)$ *lies in* $C_{Z(\overline{K}_u)}(\sigma)$ *(see* [26, Corollary 24.13]*) it follows that* $Z(K_u) = 1$ *except if* $K_u = \mathrm{SL}_2(q)$ *and* q *is odd (here* $Z(K_u) = Z_2$*) or* $K_u = \mathrm{SU}_3(q^2)$ *and* 3 *divides* $q+1$ *(here* $Z(K_u) = Z_3$*). Excluding these exceptions,* K_u *is isomorphic to its adjoint version, i.e.* $K_u \cong K_a$ *and condition (a) of Lemma 2.7 can be checked with the calculation in* [11, §13.7].

The next lemma extends an observation of [34] to the split BN-pair setting.

Lemma 2.11. *If* G *is a group with a split* BN*-pair* (H, U)*, then* $H \cap UU^-U = \{1\}$.

Proof. Let $h \in H \cap UU^-U$. Then $h \in u_1U^-u_2$, with $u_1, u_2 \in U$. Equivalently, $u_1^{-1}hu_2^{-1} = h\left(u_1^{-1}\right)^h u_2^{-1} \in U^-$. But $h\left(u_1^{-1}\right)^h u_2^{-1} \in B = HU$, and hence $h\left(u_1^{-1}\right)^h u_2^{-1} \in B \cap U^- = \{1\}$ ([10, Proposition 2.5.5(i)]). Using $H \cap U = \{1\}$ this gives $h = 1$. $\square$

Proof of Theorem 1.2. We have to show that $G = (UU^-)^2$ for each prime p and each $G \in \mathcal{L}ie(p)$. Since G satisfies the assumptions of Proposition 2.4, we can assume that G is in $\mathcal{L}ie$ of rank 1. Moreover, since there is a surjective homomorphism $\phi : K_u \to K$ which maps unipotent Sylows onto unipotent Sylows, we can assume that G is universal. A universal G in $\mathcal{L}ie$ of rank 1 satisfies $G = (UU^-)^2$ by Lemma 2.9.

By Lemma 2.11, $H \cap UU^-U = \{1\}$ and so, employing Lemma 2.1, if $H \neq 1$ we must have $\gamma_{\mathrm{cp}}^U(G) > 3$, and hence $G = (UU^-)^2$ is a minimal length cp-factorization of G by U (i.e., $\gamma_{\mathrm{cp}}^U(G) = 4$). On the other hand, if $H = 1$ then $B = H \ltimes U = U$ and it follows (see [8, Theorem 5]) that $G = UU^-U$ (i.e., $\gamma_{\mathrm{cp}}^U(G) = 3$). Moreover $H = 1$ if and only if U is self-normalizing, i.e., if U is a Carter subgroup. $\square$

3. Solvable cp-factorizations

In this section we prove Theorem 1.3. The proof is based on reducing the problem of finding an upper bound on $\gamma_{\mathrm{cp}}^{\mathrm{s}}(G)$ for a general finite[2] group G to finding an upper bound on the minimal length of a special kind of a solvable conjugate factorization of a simple non-abelian group.

Definition 3.1. *A* cp*-factorization* $G = A_1 \cdots A_k$ *of a group* G *by* $A \leq G$ *will be called a special solvable* cp*-factorization if the following conditions hold:*

(i) A *is solvable.*
(ii) A *is self-normalizing in* G*.*
(iii) *For any* $\alpha \in Aut\,(G)$ *there exists* $g \in G$ *such that* $A^\alpha = A^g$*.*

The next lemma shows the existence of special solvable cp-factorizations for any finite group G.

[2] From here to the end of the paper, all groups are assumed to be finite unless otherwise stated.

Lemma 3.2. *Let G be a group, p a prime, and let P be a Sylow p-subgroup of G. Then $A := N_G(P)$ satisfies properties (ii) and (iii) in Definition 3.1, and G is a product of some conjugates of A in G. If, in addition, A is solvable then this product is a special solvable conjugate factorization of G. Furthermore, if $p = 2$ then A is solvable so any group G has at least one special solvable conjugate factorization.*

Proof. It is well-known that as a consequence of Sylow's theorems, properties (ii) and (iii) in Definition 3.3 are satisfied by any Sylow normalizer subgroup of G (see, for instance, [28, 5.13, 5.14]). In order to show that G is a product of conjugates of A it suffices to prove that $G = A^G$. Observe that P is a Sylow p-subgroup of A^G and clearly $A^G \trianglelefteq G$. Hence, by Frattini's argument, $G = A\left(A^G\right) = A^G$. Finally, if $p = 2$ then A is solvable by the Odd Order Theorem. □

Definition 3.3. *For a finite group G we denote by $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(G)$ the minimal length of a special solvable* cp*-factorization of G. For a prime p we let $\gamma_{\mathrm{cp}}^{p}(G)$ denote the minimal length of a* cp*-factorization of G whose factors are conjugates of a solvable normalizer in G of a Sylow p-subgroup of G, if such a factorization exists, or $\gamma_{\mathrm{cp}}^{p}(G) = \infty$ otherwise.*

Note that for every prime p we have $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(G) \le \gamma_{\mathrm{cp}}^{p}(G)$ by Lemma 3.2.

3.1. **Special solvable factorizations of simple groups.** Here we obtain an upper bound on $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(G)$, where S is a simple non-abelian group. We discuss separately simple groups of Lie type, alternating groups and simple sporadic groups, and then combine the various results in Theorem 3.8.

Lemma 3.4. *If S is a simple group of Lie type of characteristic p then $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(S) = \gamma_{\mathrm{cp}}^{p}(S) = 3$.*

Proof. S is a group with a BN-pair, where B, the Borel subgroup of S is solvable and is the normalizer of a Sylow p-subgroup of S. Hence $\gamma_{\mathrm{cp}}^{p}(S) = 3$ by [8, Theorem 3]. □

Lemma 3.5. *If $S \cong A_n$ for $n \ge 5$ then $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(S) < 12\log_2(n)$.*

Proof. We first show that the symmetric group S_n is a product of less than $4\log_2(n)$ Sylow 2-subgroups, adjusting the ideas of the proof of [1, Theorem 2] to our needs. For any positive integer n set $\Omega_n := \{1, 2, ..., n\}$. Denote the minimal length of a cp-factorization of G whose factors are Sylow 2-subgroups, by $f(n)$. First we show that $f(n+1) \le f(n) + 2$. Let $A \cong S_n$ be the point stabilizer of 1, with respect to the natural action of S_{n+1} on Ω_{n+1}. Then A is a product of $f(n)$ Sylow 2-subgroups of A each of which is a subgroup of a Sylow 2-subgroup of S_{n+1}. Next we prove that there exist two Sylow 2-subgroups, P and Q of S_{n+1}, such that PQ contains elements $g_1 = 1_{S_{n+1}}, g_2, ..., g_{n+1}$ satisfying $(1)\, g_i = i$ for each $1 \le i \le n+1$ ($(1)\, g_i$ stands for the image of $1 \in \Omega_{n+1}$ under the action of $g_i \in S_{n+1}$). Note that a subset $\{g_1, ..., g_{n+1}\}$ of S_{n+1} whose elements satisfy the last condition is a right transversal of A in S_{n+1}, for if $i \ne j$ then $(1)\, g_i g_j^{-1} \ne 1$, implying $g_i g_j^{-1} \notin A$. Clearly, if PQ contains a right transversal of A in S_{n+1}, we have $APQ = S_{n+1}$, and $f(n+1) \le f(n) + 2$ follows.

Let k be the unique integer satisfying $2^k \le n+1 < 2^{k+1}$. We can choose P to be a Sylow 2-subgroup of S_{n+1} containing $\left\langle \left(1, ..., 2^k\right) \right\rangle$, and Q a Sylow 2-subgroup of S_{n+1} containing $\left\langle \left(n - 2^k + 2, ..., n+1\right) \right\rangle$. These two cyclic subgroups

act transitively on their supports, and their supports have at least one point in common. Hence PQ contains a subset $\{g_1, ..., g_{n+1}\}$ having the desired property.

Next we show that if n is even then $f(n) \le 2f(2) + f(n/2)$. In this case, Ω_n is in bijection with the set $\widetilde{\Omega}_n := \{1, 2\} \times \Omega_{n/2}$. The natural action of S_n on Ω_n induces an action of S_n on $\widetilde{\Omega}_n$. Let A be the subgroup consisting of all $g \in S_n$ such that for any $(a, b) \in \widetilde{\Omega}_n$ we have $(a, b)\, g = (a, x)$ for some $x \in \Omega_{n/2}$ and similarly, B is the subgroup of S_n preserving the second coordinate of the $\widetilde{\Omega}_n$ element. Then, $A \cong (S_{n/2})^2$ and $B \cong (S_2)^{n/2}$. By [1, Lemma 4], $S_n = BAB$. This gives $f(n) \le 2f(2) + f(n/2)$.

Using these two inequalities we prove $f(n) < 4 \log_2(n)$ by induction. If n is even then

$$f(n) \le 2 + f(n/2) < 2 + 4 \log_2(n/2) < 4 \log_2(n).$$

If n is odd, then

$$f(n) \le 2 + f(n-1) \le 4 + f((n-1)/2) < 4 + 4 \log_2((n-1)/2) < 4 \log_2(n).$$

Next we show that for $n \ge 6$ the group A_n is a product of at most $12 \log_2(n)$ Sylow 2-subgroups. The group A_n acts transitively on $P_2(\Omega_n)$ the set of all $n(n-1)/2$ subsets of Ω_n of size 2. One can check that the stabilizer of a subset of size 2 of Ω_n is isomorphic to S_{n-2}. Let H_1 and H_2 be the stabilizers of $\{1, 2\}$ and $\{n-1, n\}$ respectively. We claim that $A_n = H_1H_2H_1$. Notice that this claim together with our previous claim that S_n is a product of less than $4 \log_2(n)$ Sylow 2-subgroups, finish the proof. We have $H_2 = H_1^g$ with $g = (1, n-1)\,(2, n)$. By [8, Theorem 1 part 2 (ii)] it is sufficient to show that $\{1, 2\}H_2$ intersects every H_1 orbit O on $P_2(\Omega_n)$. Let $\{i, j\} \in O$ be arbitrary. If $\{i, j\} \cap \{n-1, n\} = \emptyset$, then there exists an $h \in H_2$ so that $\{1, 2\}h = \{i, j\}$. On the other hand, if $\{i, j\} \cap \{n-1, n\} \ne \emptyset$ then, since $n \ge 6$, there exists $h_1 \in H_1$ so that $\{i, j\}h_1 \cap \{n-1, n\} = \emptyset$, and so, since $\{i, j\}h_1 \in O$ we reduce to the previous case.

Finally, $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(A_5) = 3$ by Lemma 3.4 since $A_5 \cong PSL\,(2, 4)$ is of Lie type in characteristic 2. For $n \ge 6$ we have shown that A_n is a product of at most $12 \log_2(n)$ Sylow 2-subgroups, hence $\gamma_{\mathrm{cp}}^{2}(A_n)$ exists and satisfies $\gamma_{\mathrm{cp}}^{2}(A_n) < 12 \log_2(n)$. The claim of the lemma follows. □

Lemma 3.6. *If S is a sporadic simple group or the Tits group then upper bounds on $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(S)$ are given in the Appendix, in Table 1, under the column heading $\gamma_{\mathrm{cp}}^{p}(S) \le$. It follows that if S is a sporadic simple group or the Tits group or a simple group of Lie type then $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(S) < 4.84 \log_2 \log_2 |S|$.*

Proof. The deduction of the upper bounds in Table 1 uses several ingredients. The first one is the detailed information about the maximal subgroups of the sporadic simple groups which is available in [2]. A second ingredient is a basic inequality which relates $\gamma_{\mathrm{cp}}^{p}(G)$ to $\gamma_{\mathrm{cp}}^{p}(A)$ for $A \le G$. This and other useful relations are summarized in the following lemma.

Lemma 3.7. *Let G be a group, and p a prime divisor of $|G|$. Let P be a Sylow p-subgroup of G.*

(a) *Suppose that $A \le G$ contains P, and that $\gamma_{\mathrm{cp}}^{A}(G)$, $\gamma_{\mathrm{cp}}^{p}(G)$ and $\gamma_{\mathrm{cp}}^{p}(A)$ all exist. Then $\gamma_{\mathrm{cp}}^{p}(G) \le \gamma_{\mathrm{cp}}^{A}(G)\gamma_{\mathrm{cp}}^{p}(A)$.*
(b) *If G is an almost simple group with socle S, $|G : S|$ is not divisible by p and $\gamma_{\mathrm{cp}}^{p}(S)$ exists, then $\gamma_{\mathrm{cp}}^{p}(G) \le \gamma_{\mathrm{cp}}^{p}(S)$.*

(c) *Let $N \trianglelefteq G$. If $N \leq N_G(P)$ is solvable then $\gamma^p_{\mathrm{cp}}(G) = \gamma^p_{\mathrm{cp}}(G/N)$.*
(d) *If P is non-normal (e.g., G is simple) then $N_G(P)$ is solvable if and only if for each maximal subgroup M of G such that $|P|$ divides $|M|$, the normalizer of a Sylow p-subgroup of M is solvable.*
(e) *If G is a product of n arbitrary p-subgroups, and $N_G(P)$ is solvable then $\gamma^p_{\mathrm{cp}}(G) \leq n$.*
(f) *If G has a normal subgroup N such that N is a product of n arbitrary p-subgroups, G/N is a p-group, and $N_G(P)$ is solvable, then $\gamma^p_{\mathrm{cp}}(G) \leq n$.*

Proof. (a) By assumption, A is a product of $\gamma^p_{\mathrm{cp}}(A)$ A-conjugates of $N_A(P)$, and G is a product of $\gamma^A_{\mathrm{cp}}(G)$ G-conjugates of A. Hence G is a product of $\gamma^A_{\mathrm{cp}}(G)\gamma^p_{\mathrm{cp}}(A)$ G-conjugates of $N_A(P)$. The claim now follows from $N_A(P) \leq N_G(P)$.

(b) Since $S \trianglelefteq G$, we have that $S \cap P$ is a Sylow p-subgroup of S, and Since $|G : S|$ is not divisible by p we get $P = S \cap P$. In [17, Lemma 14], take $m = 1$, $X = G$ and $U = N_G(P)$. Then $US = N_G(P)S = G$ by the Frattini's argument, and $U \cap S = N_S(P)$. Since $1 < N_S(P) < S$ we can deduce from [17, Lemma 14], that G is a product of $h = \gamma^p_{\mathrm{cp}}(S)$ conjugates of $N_G(N_S(P))$. Now, because $S \trianglelefteq G$, $U = N_G(P)$ normalizes $U \cap S = N_S(P)$, and hence $N_G(P) \leq N_G(N_S(P))$. Using $N_G(P)S = G$ and Dedekind's argument we get:

$$N_G(N_S(P)) = N_G(N_S(P)) \cap (N_G(P)S) = N_G(P)(N_G(N_S(P)) \cap S) =$$
$$N_G(P)N_S(N_S(P)) = N_G(P)N_S(P) = N_G(P).$$

Therefore G is a product of $\gamma^p_{\mathrm{cp}}(S)$ conjugates of $N_G(P)$. Finally note that the existence of $\gamma^p_{\mathrm{cp}}(S)$ implies the solvability of $N_S(P)$ which implies, using Schreier's Conjecture, the solvability of $N_G(P)$. The claim follows.

(c) For each $A \leq G$ set $\overline{A} := AN/N$. Then, in general (without assuming $N \leq N_G(P)$) we have $\overline{N_G(P)} = N_{\overline{G}}(\overline{P})$ ([15, 3.2.8]). If $N \leq N_G(P)$ is solvable then $\overline{N_G(P)} = N_G(P)/N = N_{\overline{G}}(\overline{P})$, and $N_G(P)$ is solvable if and only if $N_{\overline{G}}(\overline{P})$ is solvable. Moreover, in this case G is a product of k conjugates of $N_G(P)$ if and only if $\overline{G}$ is a product of k conjugates of $N_{\overline{G}}(\overline{P})$. The claim follows.

(d) This follows from the fact that $N_M(P) \leq N_G(P)$ for any $M \leq G$, and from the fact that if P is non-normal, then $N_G(P)$ is contained in some maximal subgroup of G, so $N_M(P) = N_G(P)$ for some maximal subgroup M of G, which contains P.

(e) Each p-subgroup of G is contained in a Sylow p-subgroup of G which is, in turn, contained in its normalizer.

(f) By assumption $N = Q_1 \cdots Q_n$ where each Q_i is a p-subgroup. Assume, without loss of generality, $Q_n \leq P$. We have $G = NP$ because G/N is a p-group. Now $G = NP = Q_1 \cdots Q_{n-1}P$ and the claim follows from (e). □

A third and crucial ingredient is the possibility to calculate $\gamma^A_{\mathrm{cp}}(G)$ for many pairs (G, A) of interest, using the permutation character 1_A^G. If the irreducible decomposition of this character in terms of the complex irreducible characters of G is multiplicity free, one can employ a method, developed and implemented in GAP as a tool called "mfer" by T. Breuer, I. Höhler and J. Müller ([7], [6],[16] and [5]), in order to obtain the structure constants of the Hecke algebra of the double cosets of A. From these structure constants one can compute $\gamma^A_{\mathrm{cp}}(G)$ as explained in [8, Sections 2.1 and 5]. Note that the "mfer" tool can be applied to groups G where G is a simple sporadic group, as well as to some of the groups stored in the

TomLib library of [16]. The fourth ingredient are our two results from the current paper: Lemma 3.4 and Theorem 1.2. Further details on how these four ingredients are used for deducing Table 1 are given in the Appendix.

Finally, in order to prove the statement that $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(S) < 4.84 \log_2 \log_2 |S|$ holds for all simple non-abelian groups which are either of Lie type or sporadic or the Tits group, we have to find the maximum of $u(S) / \log_2 \log_2 |S|$ where $u(S)$ is the upper bound we have on $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(S)$, and S varies over the groups in question. Let S be a simple group of Lie type. Then, by Lemma 3.4, $u(S) = 3$ and $u(S) / \log_2 \log_2 |S| < 1.18$, where the value 1.18 is obtained from the minimal value 60 that $|S|$ attains. For the groups in Table 1 one gets $u(S) / \log_2 \log_2 |S| < 4.84$, where the maximum is realized by the HN group. $\square$

Theorem 3.8. *Let S be a simple non-abelian group. Then $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(S) < c \log_2 \log_2 |S|$, where $0 < c \leq 12$ is a universal constant.*

Proof. For $S \cong A_n$ assume $n \geq 6$ (A_5 is treated as a simple group of Lie type). Using $n!/2 \geq (n/e)^n$ which holds for all $n \geq 1$, gives

$$\log_2(|S|) = \log_2(n!/2) \geq \log_2((n/e)^n) = n \log_2(n/e),$$

and, $\log_2 \log_2(|S|) \geq \log_2(n) + \log_2 \log_2(n/e)$. Since $n \geq 6$, we have $n/e > 2$ and $\log_2 \log_2(n/e)$ is positive so $\log_2(n) < \log_2 \log_2(|S|)$. Thus, by Lemma 3.5, $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(S) < 12 \log_2(n) < 12 \log_2 \log_2(|S|)$. If S is sporadic or of Lie type we have $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(S) \leq 4.84 \log_2 \log_2 |S|$ by Lemma 3.6. Combining the two cases gives the claim of the theorem. $\square$

3.2. **Reduction to special solvable** cp**-factorizations.** In this section we reduce the analysis of $\gamma_{\mathrm{cp}}^{\mathrm{s}}$ to that of $\gamma_{\mathrm{cp}}^{\mathrm{ss}}$ for simple groups, and this reduction enables us to use Theorem 3.8 for proving Theorem 1.3.

Lemma 3.9. *Let $G = T_1^{r_1} \times \cdots \times T_m^{r_m}$ where the T_i's are pairwise non-isomorphic non-abelian simple groups, and $r_1, ..., r_m$ are positive integers. Then*

$$\gamma_{\mathrm{cp}}^{\mathrm{ss}}(G) \leq \max\left\{\gamma_{\mathrm{cp}}^{\mathrm{ss}}(T_1), ..., \gamma_{\mathrm{cp}}^{\mathrm{ss}}(T_m)\right\}.$$

Proof. For each $1 \leq i \leq m$ set $k_i := \gamma_{\mathrm{cp}}^{\mathrm{ss}}(T_i)$. By assumption, for each $1 \leq i \leq m$ there exists $B_{i1} < T_i$ satisfying Definition 3.1, and $T_i = B_{i1} \cdots B_{ik_i}$ where B_{ij} is conjugate in T_i to B_{i1} for all $1 \leq j \leq k_i$. Set $k := \max\{k_1, ..., k_m\}$. We can assume that the special solvable conjugate factorizations of the T_i are all of equal length k, since for each $1 \leq i \leq m$ we can add subgroups B_{ij} with $k_i + 1 \leq j \leq k$, chosen arbitrarily from the conjugates of B_{i1} in T_i. Clearly $T_i = B_{i1} \cdots B_{ik}$. We claim that $T_i^{r_i} = B_{i1}^{r_i} \cdots B_{ik}^{r_i}$ is a special solvable conjugate factorization of $T_i^{r_i}$. It is easy to see that each $B_{ij}^{r_i}$ is solvable, being a direct product of solvable groups, and that each $B_{ij}^{r_i}$ is conjugate in $T_i^{r_i}$ to $B_{i1}^{r_i}$ because each B_{ij} is conjugate in T_i to B_{i1}. Similarly, $B_{i1}^{r_i}$ is self-normalizing in $T_i^{r_i}$, because B_{i1} is self-normalizing in T_i. In order to verify condition (iii) of Definition 3.3, recall that $Aut\,(T_i^{r_i}) \cong Aut\,(T_i)^{r_i} \rtimes S_{r_i}$ where the symmetric group S_{r_i} permutes the r_i direct factors of $Aut\,(T_i)^{r_i}$ according to its natural action on $\{1, ..., r_i\}$ ([28, 9.24]). Thus S_{r_i} normalizes $B_{i1}^{r_i}$. Let $\alpha \in Aut\,(T_i^{r_i})$. We have $\alpha = g\,(\alpha_1, ..., \alpha_{r_i})$ where $\alpha_j \in Aut\,(T_i)$, $1 \leq j \leq r_i$ and $g \in S_{r_i}$. Since g normalizes $B_{i1}^{r_i}$ we get $(B_{i1}^{r_i})^{\alpha} = B_{i1}^{\alpha_1} \times \cdots \times B_{i1}^{\alpha_{r_i}}$. Now we can use the fact that B_{i1} satisfies condition (iii) of Definition 3.3, as a subgroup of T_i.

Next define for each $1 \le j \le k$, $B_j := \prod_{i=1}^{m} B_{ij}^{r_i}$ (a direct product). We have $G = B_1 \cdots B_k$, and again we claim that this is a special solvable conjugate factorization. The proof relies on the previous claim, namely, that $T_i^{r_i} = B_{i1}^{r_i} \cdots B_{ik}^{r_i}$ is a special solvable conjugate factorization, and proceeds in the same way where for showing that B_1 satisfies condition (iii) of Definition 3.3, we use the fact that $Aut\,(G) = Aut\,(T_1^{r_1}) \times \cdots \times Aut\,(T_m^{r_m})$, which follows from the fact that the T_i's are pairwise non-isomorphic non-abelian simple groups ([28, 9.25]).

Finally, since $G = B_1 \cdots B_k$ is a special solvable conjugate factorization, we get $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(G) \le k$ which is what we wanted to prove. $\square$

Now we state and prove the main reduction argument.

Lemma 3.10. *Let G be a finite group and let $N \trianglelefteq G$. Then*

$$\gamma_{\mathrm{cp}}^{\mathrm{s}}(G) \le \gamma_{\mathrm{cp}}^{\mathrm{ss}}(N) + \gamma_{\mathrm{cp}}^{\mathrm{s}}(G/N).$$

Proof. Set $t := \gamma_{\mathrm{cp}}^{\mathrm{s}}(G/N)$. Then, by definition of $\gamma_{\mathrm{cp}}^{\mathrm{s}}(G/N)$, there exists $H \le G$ and $N \le H$ such that H/N is solvable, and there exist t subgroups $H_1, \ldots, H_t$ of G, all containing N, such that $G/N = (H_1/N) \cdots (H_t/N)$, and H_i/N is conjugate to H/N in G/N for each $1 \le i \le t$. It follows that H_i is conjugate to H in G for all $1 \le i \le t$, and $G = H_1 \cdots H_t$.

Set $k := \gamma_{\mathrm{cp}}^{\mathrm{ss}}(N)$. By definition of $\gamma_{\mathrm{cp}}^{\mathrm{ss}}(N)$, there exists $B \le N$ satisfying (i)-(iii) in Definition 3.1 and $N = B_1 \cdots B_k$, where each B_i is conjugate to B in N. We claim that $H = N_H\,(B)\,N$. First note that both $N_H\,(B)$ and N are subgroups of H so $N_H\,(B)\,N \le H$. For the reverse inclusion let $h \in H$ be arbitrary. Since $N \trianglelefteq H$, h acts on N as an automorphism, and therefore, by property (iii) in Definition 3.1, there exists $n \in N$ such that $B^h = B^n$ from which it follows that $hn^{-1} \in N_H\,(B)$. Hence $h = \left(hn^{-1}\right) n \in N_H\,(B)\,N$.

Now $H = N_H\,(B)\,N$ implies that $H/N = N_H\,(B)\,N/N \cong N_H\,(B)\,/B$ (by Definition 3.1.(ii)). But since both H/N and B are solvable, we get that $N_H\,(B)$ is solvable.

For each $1 \le i \le t$ let $g_i \in G$ be such that $H_i = H^{g_i}$, and for each $1 \le j \le k$ let $n_j \in N$ be such that $B_j = B^{n_j}$. Using the above we get:

$$\begin{gathered} G = H_1 \cdots H_t = H^{g_1} \cdots H^{g_t} = (N_H\,(B)\,N)^{g_1} \cdots (N_H\,(B)\,N)^{g_t} = \\ = (N_H\,(B))^{g_1} \cdots (N_H\,(B))^{g_t}\, N = (N_H\,(B))^{g_1} \cdots (N_H\,(B))^{g_t}\, B_1 \cdots B_k = \\ = (N_H\,(B))^{g_1} \cdots (N_H\,(B))^{g_t}\, B^{n_1} \cdots B^{n_k} = \\ = (N_H\,(B))^{g_1} \cdots (N_H\,(B))^{g_t}\, (N_H\,(B))^{n_1} \cdots (N_H\,(B))^{n_k}\,. \end{gathered}$$

Since $N_H\,(B)$ is solvable this implies that $\gamma_{\mathrm{cp}}^{\mathrm{s}}(G) \le k + t$ as claimed. $\square$

Our next definition is required for the application of Lemma 3.10. We denote by $R\,(G)$ the solvable radical of G and by $\mathrm{soc}\,(G)$ the socle of G.

Definition 3.11. *Let G be a finite group.* The non-abelian socle series *of G is the unique normal series $R\,(G) = H_1 \le \ldots \le H_t = G$ of G which satisfies the following conditions:*

(i) *for all $1 \le i \le (t-1)/2$ we have $H_{2i+1}/H_{2i} = R\,(G/H_{2i})$,*
(ii) *for all $1 \le i \le t/2$ we have $H_{2i}/H_{2i-1} = \mathrm{soc}\,(G/H_{2i-1})$.*

The number $\lfloor t/2 \rfloor$ will be called the non-abelian socle length *of G.*

In the sequel we will denote $N_i := H_{2i}/H_{2i-1} = \mathrm{soc}\,(G/H_{2i-1})$, and n_i will stand for the number of simple non-abelian direct factors of N_i for all $1 \leq i \leq t/2$. Observe that the uniqueness of the non-abelian socle series of G is a consequence of the uniqueness of the solvable radical and the socle of any given finite group. Moreover, for all $1 \leq i \leq t/2$ we have $R\,(G/H_{2i-1}) = 1$. This is clear for $i = 1$, and for $i \geq 2$ we have $G/H_{2i-1} \cong (G/H_{2i-2})\,/\,(H_{2i-1}/H_{2i-2})$ and now we can use $H_{2i-1}/H_{2i-2} = R\,(G/H_{2i-2})$. Since $R\,(G/H_{2i-1}) = 1$ we get that N_i is a non-trivial direct product of non-abelian simple groups. As a result, the inclusion $H_{2i-1} \leq H_{2i}$ is always strict, while the inclusion $H_{2i} \leq H_{2i+1}$ need not be strict. Finally note that the non-abelian socle length of G is zero if and only if G is solvable.

Corollary 3.12. *Let G be a non-trivial finite group whose non-abelian socle length is $m \geq 0$. For each $1 \leq i \leq m$ pick a simple non-abelian direct factor T_i of N_i such that $\gamma^{\mathrm{ss}}_{\mathrm{cp}}(T_i)$ is maximal compared to any other factor of N_i. Then*

$$\gamma^{\mathrm{s}}_{\mathrm{cp}}(G) \leq 1 + \sum_{i=1}^{m} \gamma^{\mathrm{ss}}_{\mathrm{cp}}(T_i). \tag{3.1}$$

Proof. By induction on $m \geq 0$. If $m = 0$ then G is solvable and so $\gamma^{\mathrm{s}}_{\mathrm{cp}}(G) = 1$. Suppose $m > 0$. Then $\gamma^{\mathrm{s}}_{\mathrm{cp}}(G) \leq \gamma^{\mathrm{s}}_{\mathrm{cp}}(G/R\,(G))$. In fact equality holds since if $G = A_1 \dots A_k$ is a solvable cp-factorization then so is $G = (A_1 R\,(G)) \dots (A_k R\,(G))$. Moreover, if $R\,(G) = H_1 \leq \dots \leq H_t = G$ is the non-abelian socle series of G, then $1 = H_1/R\,(G) \leq \dots \leq H_t/R\,(G) = G/R\,(G)$ is the non-abelian socle series of $G/R\,(G)$. We have $R\,(G/R\,(G)) = 1$ and $N_1 = H_2/R\,(G)$. Hence, by Lemma 3.10 we have $\gamma^{\mathrm{s}}_{\mathrm{cp}}(G) = \gamma^{\mathrm{s}}_{\mathrm{cp}}(G/R\,(G)) \leq \gamma^{\mathrm{ss}}_{\mathrm{cp}}(N_1) + \gamma^{\mathrm{s}}_{\mathrm{cp}}((G/R\,(G))\,/\,(H_2/R\,(G)))$. Using $(G/R\,(G))\,/\,(H_2/R\,(G)) \cong G/H_2$, we obtain $\gamma^{\mathrm{s}}_{\mathrm{cp}}(G) \leq \gamma^{\mathrm{ss}}_{\mathrm{cp}}(N_1) + \gamma^{\mathrm{s}}_{\mathrm{cp}}\,(G/H_2)$. By Lemma 3.9, $\gamma^{\mathrm{ss}}_{\mathrm{cp}}(N_1) \leq \gamma^{\mathrm{ss}}_{\mathrm{cp}}(T_1)$, and since the non-abelian socle length of G/H_2 is $m-1$, we have by induction $\gamma^{\mathrm{s}}_{\mathrm{cp}}(G/H_2) \leq 1 + \sum\limits_{i=2}^{m} \gamma^{\mathrm{ss}}_{\mathrm{cp}}(T_i)$. The claim follows. $\square$

Theorem 3.8 provides an upper bound on each term in the sum $\sum_{i=1}^{m} \gamma^{\mathrm{ss}}_{\mathrm{cp}}(T_i)$ appearing on the r.h.s. of Inequality 3.1. The last ingredient of the proof of Theorem 1.3 is an upper bound on the number of terms in this sum which is equal to the non-abelian socle length of G. Recall that for any finite group H there exists the least integer n, customarily denoted $\mu(H)$, so that H embeds in the symmetric group S_n. In other words, $\mu\,(H)$ is the minimal degree of a faithful permutation representation of H. We will make use of the following properties of this quantity. If $H_1 \leq H$ then $\mu\,(H_1) \leq \mu\,(H)$ (immediate from the definition). If $N = T_1 \times \cdots \times T_k$ where T_i simple non-abelian for each $1 \leq i \leq k$ then $\mu\,(N) = \sum\limits_{i=1}^{k} \mu\,(T_i)$ ([14, Theorem 3.1]). If $N \trianglelefteq H$ and $R\,(H/N) = 1$ then $\mu\,(H/N) \leq \mu\,(H)$ ([23, Theorem 1]). If T is simple non-abelian then $\mu\,(T) \geq 5$ (since all subgroups of S_n are solvable if $n < 5$).

Lemma 3.13. *Let G be a non-solvable group and let $R\,(G) = H_1 \leq \dots \leq H_t = G$ be the non-abelian socle series of G. Then, for each $i > 1$, $\mu\,(G/H_{2i-1}) \leq n_{i-1}$.*

Proof. It is clearly sufficient to prove this for the case $i = 2$. So we will prove $\mu\,(G/H_3) \leq n_1$. Since G/H_1 has a trivial solvable radical it acts faithfully by conjugation on $N_1 = soc\,(G/H_1) = H_2/H_1$ and so embeds in $Aut\,(N_1)$. Now $N_1 = T_1^{r_1} \times \cdots \times T_m^{r_m}$ where the T_i's are pairwise non-isomorphic non-abelian simple groups, and $r_1, ..., r_m$ are positive integers ($\sum_{i=1}^{m} r_i = n_1$). We have $Aut\,(N_1) =$

$Aut\,(T_1^{r_1}) \times \cdots \times Aut\,(T_m^{r_m})$ and $Aut\,(T_i^{r_i}) \cong Aut\,(T_i)^{r_i} \rtimes S_{r_i}$ where the symmetric group S_{r_i} permutes the r_i direct factors of $Aut\,(T_i)^{r_i}$ according to its natural action on $\{1, ..., r_i\}$ (see [28, 9.25]). Now, the image of G/H_1 in $Aut\,(N_1)$ contains $Inn\,(T_1^{r_1}) \times \cdots \times Inn\,(T_m^{r_m}) = (Inn\,(T_1))^{r_1} \times \cdots \times (Inn\,(T_m))^{r_m}$ which is, in fact, the image of N_1 so

$$\begin{aligned}(G/H_1)\,/N_1 = (G/H_1)\,/\,(H_2/H_1) \cong G/H_2 \precsim Aut\,(N_1)\,/\prod_{i=1}^{m}(Inn\,(T_i))^{r_i}\\ \cong \prod_{i=1}^{m} Out\,(T_i)^{r_i} \rtimes S_{r_i},\end{aligned}$$

where $\prod_{i=1}^{m}$ is direct, $Out\,(T_i) := Aut\,(T_i)\,/Inn\,(T_i)$, and $\precsim$ denotes embedding. Set $A := \prod_{i=1}^{m} Out\,(T_i)^{r_i} \rtimes S_{r_i}$, $B := \prod_{i=1}^{m} Out\,(T_i)^{r_i}$ and $S := \prod_{i=1}^{m} S_{r_i} \leq S_{n_1}$. We have $A = BS$, and $B \trianglelefteq A$. Furthermore, B is solvable by Schreier's conjecture. Hence $B \leq R\,(A)$. Therefore $A/R\,(A) = SR\,(A)\,/R\,(A) \cong S/\,(S \cap R\,(A))$. Since $R\,(A/R\,(A)) = 1$ we have $R\,(S/\,(S \cap R\,(A))) = 1$. Thus, by [23, Theorem 1],

$$\mu\,(A/R\,(A)) = \mu\,(S/\,(S \cap R\,(A))) \leq \mu\,(S) \leq \mu\,(S_{n_1}) = n_1.$$

Now, identifying G/H_2 with its embedding in A, we have that $(G/H_2)\,R\,(A)\,/R\,(A)$ is a subgroup of $A/R\,(A)$ and so $\mu\,((G/H_2)\,R\,(A)\,/R\,(A)) \leq \mu\,(A/R\,(A))$. On the other hand,

$$(G/H_2)\,R\,(A)\,/R\,(A) \cong (G/H_2)\,/\,((G/H_2) \cap R\,(A))\,.$$

Set $D := (G/H_2) \cap R\,(A) \leq R\,(G/H_2)$. By an isomorphism theorem we have $((G/H_2)\,/D)\,/\,(R\,(G/H_2)\,/D) \cong (G/H_2)\,/R\,(G/H_2)$. Hence, by [23, Theorem 1],:

$$\begin{aligned}\mu\,((G/H_2)\,/R\,(G/H_2)) \leq \mu\,((G/H_2)\,/D) = \mu\,((G/H_2)\,R\,(A)\,/R\,(A))\\ \leq \mu\,(A/R\,(A)) \leq n_1.\end{aligned}$$

On the other hand

$$(G/H_2)\,/R\,(G/H_2) = (G/H_2)\,/\,(H_3/H_2) \cong G/H_3,$$

and the claim $\mu\,(G/H_3) \leq n_1$ follows. □

Lemma 3.14. *Let G be a non-solvable group, and let m be the non-abelian socle length of G. Then $5n_i \leq n_{i-1}$ for all $2 \leq i \leq m$.*

Proof. Let $R\,(G) = H_1 \leq \ldots \leq H_t = G$ be the non-abelian socle series of G. By the preceding remarks, $N_i = soc\,(G/H_{2i-1}) = T_{i1} \times \cdots \times T_{in_i}$ for all $1 \leq i \leq m$, where each T_{ij} is a non-abelian simple group. We have:

$$\mu\,(N_i) = \sum_{j=1}^{n_i} \mu\,(T_{ij}) \geq 5n_i.$$

On the other hand, by Lemma 3.13, $\mu\,(N_i) \leq \mu\,(G/H_{2i-1}) \leq n_{i-1}$. Thus $5n_i \leq n_{i-1}$ for all $2 \leq i \leq m$. □

Corollary 3.15. *Let G be a non-solvable group, and let m be the non-abelian socle length of G. Then $m < (1/\log_2 5)\log_2\log_2|G|_{\mathrm{nab}}$.*

Proof. By the previous lemma $5n_i \le n_{i-1}$ for all $2 \le i \le m$. Since $n_m \ge 1$ we get by induction, $n_i \ge 5^{m-i}$ for all $1 \le i \le m$, and hence the total number of non-abelian composition factors of G satisfies

$$\sum_{i=1}^{m} n_i \ge \sum_{i=1}^{m} 5^{m-i} = \sum_{i=0}^{m-1} 5^i = \frac{5^m - 1}{4}.$$

Each non-abelian composition factor of G is of size at least $|A_5| = 60 > 2^5$ so

$$|G|_{\mathrm{nab}} \ge 60^{\frac{5^m-1}{4}} > 2^{\frac{5}{4}(5^m-1)} \ge 2^{5^m},$$

which gives $m < (1/\log_2 5)\log_2\log_2 |G|_{\mathrm{nab}}$. □

Proof of Theorem 1.3. By Corollary 3.12 we have $\gamma^{\mathrm{s}}_{\mathrm{cp}}(G) \le 1 + \sum_{i=1}^{m} \gamma^{\mathrm{ss}}_{\mathrm{cp}}(T_i)$. Since T_i is a non-abelian composition factor we have $|T_i| \le |G|_{\mathrm{nab}}$. Hence, by Theorem 3.8, $\gamma^{\mathrm{ss}}_{\mathrm{cp}}(T_i) < c\log_2\log_2|G|_{\mathrm{nab}}$ for all $1 \le i \le m$. Substituting in the previous inequality we get $\gamma^{\mathrm{s}}_{\mathrm{cp}}(G) \le 1 + mc\log_2\log_2|G|_{\mathrm{nab}}$. Finally, $c \le 12$ by Theorem 3.8, and $m < (1/\log_2 5)\log_2\log_2|G|_{\mathrm{nab}}$ by Corollary 3.15, so the claim of the theorem holds with $c_S \le 12/\log_2 5$. □

4. Nilpotent cp-factorizations

In this section we prove Theorem 1.4. The proof relies on Theorem 1.6 which is of independent interest. Hence we begin with the latter.

4.1. cp**-factorizations of affine primitive groups.** Recall that a group G is said to be primitive if it admits a maximal subgroup H which is core-free: $H_G = \bigcap_{g\in G} H^g = \{1\}$. If G is an affine primitive permutation group, then it has exactly one minimal normal subgroup V, which is abelian so $V \cong C_p^n$ for some prime p and some natural number n. Moreover $G = VH$ and, viewing V as the vector space over $\mathbb{F}_p$, then H acts by conjugation irreducibly as a group of linear transformations on V. When convenient we will use additive notation for V.

Lemma 4.1. *Let G be an affine primitive permutation group with point stabilizer H and minimal normal subgroup $V \cong C_p^n$. Let $h \in H$ and $v \in V$. Set $w := v^{h^{-1}} - v$ and $k := \lceil \log_2 p \rceil$. Then $\langle w \rangle$ is contained in a product of $k+1$ conjugates of H.*

Proof. We can assume $w \ne 0_V = 1_G$ for which the claim clearly holds. Then w is of order p, and any element of $\langle w \rangle$ is of the additive form sw where the integer s satisfies $0 \le s \le p-1$. Since $k := \lceil \log_2 p \rceil$, the base 2 representation of s takes the form $s = \sum_{j=0}^{k-1} b_j 2^j$ ($b_j \in \{0,1\}$ for all $0 \le j \le k-1$). Now note that $w = v^{h^{-1}} - v = v^{-1}hvh^{-1} \in H^vH$. Similarly, for any $c \in \mathbb{F}_p$ we have $cw = (cv)^{h^{-1}} - cv \in H^{cv}H$. Thus, identifying the powers 2^j with elements of $\mathbb{F}_p$, we see that $sw \in (H^vH)\left(H^{2v}H\right)\left(H^{2^2v}H\right)\cdots\left(H^{2^{k-1}v}H\right)$, for any $0 \le s \le p-1$, where we pick 0_V from the j-th factor $\left(H^{2^jv}H\right)$ in the product if $b_j = 0$ and 2^jw if $b_j = 1$. However, also note that since V is abelian, $\left(H^{2^jv}H\right) \cap V$ is invariant under conjugation by any element of V. Hence, for any choice of $u_0, \ldots, u_{k-2} \in V$ we have

$$sw \in \Pi_H := (H^vH)^{u_0}\left(H^{2v}H\right)^{u_1}\left(H^{2^2v}H\right)^{u_2}\cdots\left(H^{2^{k-2}v}H\right)^{u_{k-2}}\left(H^{2^{k-1}v}H\right).$$

Finally, for the choice $u_{k-2} = 2^{k-1}v$, $u_{k-3} = u_{k-2} + 2^{k-2}v$ and in general $u_{k-j} = u_{k-j+1} + 2^{k-j+1}v$ for all $2 \leq j \leq k$ where $u_{k-1} := 0_V$, we get that Π_H is equal to a product of $k+1$ conjugates of H. □

Lemma 4.2. *For each prime number p define $f(p) := \lceil \log_2 p \rceil / \log_2 p$. Then $f(p)$ has a global maximum at $p = 5$. Consequently*

$$\lceil \log_2 p \rceil \leq (3/\log_2 5) \log_2 p, \text{ for every prime } p. \tag{4.1}$$

Proof. First check that $1 + 1/\log_2 11 < 1.29 < 3/\log_2 5$. Then, using this, we get:

$$f(p) \leq (\log_2 p + 1)/\log_2 p = 1 + 1/\log_2 p < 3/\log_2 5 = f(5), \forall p \geq 11,$$

and for $p = 2, 3, 7$ we verify explicitly that $f(p) < f(5)$. Hence $f(p)$ has a global maximum $f(5) = 3/\log_2 5$ at $p = 5$. Finally, $\lceil \log_2 p \rceil = f(p) \log_2 p \leq f(5) \log_2 p$. □

Proof of Theorem 1.6. Using the notation introduced at the beginning of Subsection 4.1, $\log_2 |G : H| = \log_2 |V| = \log_2 p^n = n \log_2 p$. Using Inequality 4.1, we obtain:

$$1 + n\lceil \log_2 p \rceil \leq 1 + (3/\log_2 5) n \log_2 p = 1 + (3/\log_2 5) \log_2 |G : H|.$$

Thus, it is enough to show that G is a product of at most $1+ n\lceil \log_2 p \rceil$ conjugates of H.

Fix a non-zero vector $v \in V$. If v is central in G then $V = \langle v \rangle$ by minimality of V. It follows that H is a non-trivial normal subgroup of $HV = G$ since V is central - a contradiction to H being core-free. Therefore v is not central, and there is some $h \in H$ with $v^{h^{-1}} \neq v$. Set $w := v^{h^{-1}} - v$.

We claim that there are n elements $h_1, \dots, h_n \in H$ such that $B := \{w^{h_1}, \dots, w^{h_n}\}$ is a vector space basis of $V = C_p^n$. Note that since $w \neq 0_V$, this claim is immediate for $n = 1$, and hence we assume $n \geq 2$. Suppose by contradiction that $1 \leq m < n$ is the maximal integer such that there exist $h_1, h_2, \dots, h_m \in H$ for which $B = \{w^{h_1}, \dots, w^{h_m}\}$ is linearly independent. It follows that for any $h \in H$, $w^h \in \mathit{Span}(B)$. Thus $\mathit{Span}(B) = \mathit{Span}\left(\{w^h | h \in H\}\right)$. This shows that $\mathit{Span}(B)$ is a proper non-trivial H-invariant subspace of V, contradicting the fact that H acts irreducibly on V. Thus there exists a basis of V of the form $B := \{w^{h_1}, \dots, w^{h_n}\}$.

For each $v \in V$ there exist $s_1, ..., s_n \in \mathbb{F}_p$ for which $v = \Sigma_{i=1}^n s_i w^{h_i}$. Applying Lemma 4.1 to each w^{h_i} separately, we get that each $v \in V$ belongs to $\Pi_1 \cdots \Pi_n$, where each Π_i is a product of $\lceil \log_2 p \rceil + 1$ conjugates of H. But, as in the proof of Lemma 4.1, this shows that $V \subseteq \Pi_1^{u_1} \cdots \Pi_{n-1}^{u_{n-1}} \Pi_n$ for any choice of $u_1, ..., u_{n-1} \in V$, and one can choose these elements so that the product $\Pi_1^{u_1} \cdots \Pi_{n-1}^{u_{n-1}} \Pi_n$ is a product of at most $n\lceil \log_2 p \rceil + 1$ conjugates of H. □

4.2. cp**-factorizations of solvable groups by Carter subgroups.** Recall that $C \leq G$ is a Carter subgroup of G if C is nilpotent and self normalizing.

Lemma 4.3. *Let G be a solvable group. Then*

(a) *There exists a Carter subgroup of G.*
(b) *There is a unique conjugacy class of Carter subgroups in G.*
(c) *If C is a Carter subgroup of G then C is a maximal nilpotent subgroup of G, that is, if $C < H \leq G$, then H is not nilpotent.*
(d) *If C is a Carter subgroup of G and $N \trianglelefteq G$ then CN/N is a Carter subgroup of G/N.*

(e) *If C is a Carter subgroup of G then C is Carter subgroup of H for any $C \leq H \leq G$.*

Proof. For (a)-(d) see [9], and [21, Theorem 12.2(b) and Lemma 12.3]. For (e) note that since C is self-normalizing in G it is self-normalizing in any subgroup of G containing C. □

Lemma 4.4. *Let G be a solvable group and let C be a Carter subgroup of G. Then G is a product of conjugates of C.*

Proof. It is enough to show that $C^G = G$. Set $N := C^G$. Note that C is a Carter subgroup of N. For any $g \in G$ we have $C^g \in N$ is a self normalizing nilpotent subgroup of N. Hence C^g is a Carter subgroup of N and hence there exists $n \in N$ such that $C^g = C^n$. It follows that gn^{-1} normalizes C and therefore $gn^{-1} \in C \leq N$. Hence $g \in N$ implying $G = N$. □

Definition 4.5. *Let G be a finite solvable group. We denote by $\gamma_{\text{cp}}^{\text{c}}(G)$ the minimal length of a* cp*-factorization of G by a Carter subgroup.*

Note that a nilpotent group G is equal to its own Carter subgroup and hence, for G nilpotent, $\gamma_{\text{cp}}^{\text{c}}(G) = 1$. Clearly $\gamma_{\text{cp}}^{\text{n}}(G) \leq \gamma_{\text{cp}}^{\text{c}}(G)$.

Lemma 4.6. *Let G be a solvable group and let C be a Carter subgroup of G. Let $N \trianglelefteq G$ be such that N is contained in C. Then $\gamma_{\text{cp}}^{\text{c}}(G) = \gamma_{\text{cp}}^{\text{c}}(G/N)$.*

Proof. It is clear that if N is contained in C then it is contained in every conjugate of C. Suppose that $G = C_1 \cdots C_k$ where C_i is a conjugate of C for all $1 \leq i \leq k$. Then $\overline{G} = \overline{C_1} \cdots \overline{C_k}$, where, for any $A \leq G$ we denote $\overline{A} := AN/N$, and each $\overline{C_i}$ is a Carter subgroup of $\overline{G}$. Conversely, if $\overline{G} = \overline{C_1} \cdots \overline{C_k}$, where the $\overline{C_i}$ are Carter subgroups of $\overline{G}$, then, by assumption, the full preimage of $\overline{C_i}$ in G is a Carter subgroup C_i of G and we can conclude that $G = C_1 \cdots C_k$. The claim follows. □

Proof of Theorem 1.4. The proof is by induction on $|G|$. Let C be a Carter subgroup of G. If G is nilpotent then $G = C$, $\gamma_{\text{cp}}^{\text{c}}(G) = 1$, and the claim clearly holds. Hence we can assume that G is non-nilpotent. Let N be a minimal normal subgroup of G. For any $A \leq G$ denote $\overline{A} := AN/N$. Then $\overline{G} = \overline{C_1} \cdots \overline{C_k}$, where each $\overline{C_i}$ is a Carter subgroup of $\overline{G}$, and $k = \gamma_{\text{cp}}^{\text{c}}(\overline{G})$. By Lemma 4.3(d), the full preimage of $\overline{C_i}$ in G is C_iN where C_i is a Carter subgroup of G, and we get $G = C_1 \cdots C_kN$. If $k > 1$, C_kN is proper in G. By Lemma 4.3(e) C_k is a Carter subgroup of C_kN and hence we get by induction that C_kN is a product of $\gamma_{\text{cp}}^{\text{c}}(C_kN) \leq c_A \log_2(|C_kN : C_k|) + 1$ conjugates of C_k. Since C_k is conjugate to C and N is normal we have $|C_kN : C_k| = |CN : C|$. Therefore

$$
\begin{aligned}
\gamma_{\text{cp}}^{\text{c}}(G) &\leq k - 1 + c_A \log_2(|C_kN : C_k|) + 1 \\
&= \gamma_{\text{cp}}^{\text{c}}(\overline{G}) + c_A \log_2(|CN : C|) \\
&\leq c_A \log_2(|G/N : CN/N|) + 1 + c_A \log_2(|CN : C|) \\
&= c_A \log_2(|G : C|) + 1,
\end{aligned}
$$

and the claim is proved. Hence we can assume $k = 1$.

In this case we have $G = CN$, where C is a Carter subgroup of G and N is a minimal normal subgroup of G. Since G is solvable, N is elementary abelian and in particular, $|N| = p^n$ for some prime p and some positive integer n. Suppose that C contains a non-trivial normal subgroup L of G. By Lemma 4.6, $\gamma_{\text{cp}}^{\text{c}}(G) = \gamma_{\text{cp}}^{\text{c}}(G/L)$

and $G/L = (C/L)\,N$ and N is minimal normal in G/L. Thus we can assume that C is core-free. Under this assumption $C_G(N) = N$. Indeed, $N \leq C_G(N)$ because N is abelian so by Dedekind's law, $C_G(N) = C_G(N) \cap (NC) = N\,(C_G(N) \cap C)$. Since $C_G(N) \trianglelefteq G$ we get that C normalizes $C_G(N) \cap C$. Moreover, N centralizes $C_G(N)$ hence it normalizes $C_G(N) \cap C$. Thus we proved that $C_G(N) \cap C \trianglelefteq G$. Since C is core-free, we get $C_G(N) \cap C = 1$ and $C_G(N) = N$. Finally, since G is solvable, G is primitive iff it has a self-centralizing minimal normal subgroup ([13, Proposition A.15.8(b)]). Thus we can conclude that G is primitive and C is maximal and non-normal. Now apply Theorem 1.6, with $H = C$. □

Appendix

Table 1 lists, for each sporadic simple group S including the Tits group ${}^2F_4(2)'$, an upper bound on $\gamma^p_{\mathrm{cp}}(S)$ (column heading $\gamma^p_{\mathrm{cp}}(S) \leq$) for a specified prime p. Under column heading p^α the maximal power of p dividing $|S|$ is given. Under the column heading A we specify a subgroup $A < S$ on which the bound is based, using ATLAS notation ([2]). We have verified, using Lemma 3.7 (d) and sometimes a MAGMA computation ([4]), that $N_S(P)$, the normalizer in S of some Sylow p-subgroup P of S is solvable. For each A in the table we have $\gamma^A_{\mathrm{cp}}(S) = 3$ - this was verified using the "mfer" tool [6] (see Subsection 3.1). In all cases, with a few exceptions detailed below (all associated with $p = 2$), A contains a Sylow p-subgroup of S. For $S = M_{11}, J_1$, we have $P \leq A \leq N_S(P)$ so the bound is exact and $\gamma^p_{\mathrm{cp}}(S) = 3$. For the other cases the bound is derived using Lemma 3.7 (a) and a bound on $\gamma^p_{\mathrm{cp}}(A)$ (when $\gamma^p_{\mathrm{cp}}(S) \leq 9$, we have $\gamma^p_{\mathrm{cp}}(A) = 3$). The determination of the bound on $\gamma^p_{\mathrm{cp}}(A)$ uses a variety of means: Lemma 3.4, information on subgroups of A from [2], an application of the "mfer" tool to A, and previous results from the table. For the $S = B$, where the bound is 12, we have deduced $\gamma^2_{\mathrm{cp}}(A) \leq 4$ from Theorem 1.2. In this as well as in the case of $S = M$, the argument relies on Lemma 3.7 (e),(f), and hence A need not contain a Sylow 2-subgroup of S.

Remarks for Table 1:

(1) A Sylow 2-subgroup of A is self-normalizing of index 3, hence $\gamma^2_{\mathrm{cp}}(A) = 3$.

(2) A Tomlib mfer calculation shows that $L_2(16)$ is a product of three Sylow 5-subgroup normalizers (structure D_{30}). Hence $L_2(16):2$ is a product of three Sylow 5-subgroup normalizers (structure $D_{10} \times S_3$).

(3),(4),(6) A is a group of Lie type hence it is a product of three Sylow 2-subgroup normalizers. A MAGMA computation shows that the Sylow 2-subgroup of A is self-normalizing. Therefore S is a product of nine conjugates of a 2-subgroup and hence it is a product of nine Sylow 2-subgroup normalizers.

(5) $2.HS.2$ is a central extension of $HS.2$ hence the order 2 center is contained in the Sylow 11-subgroup normalizer of $2.HS.2$.

S	A	p^{α}	$\gamma_{\mathrm{cp}}^{p}(S) \leq$	Remarks
M_{11}	$11:5$	11	3	
M_{12}	M_{11}	11	9	
J_1	$2^3:7:3$	2^3	3	
M_{22}	$L_2(11)$	11	9	
J_2	$U_3(3)$	3^3	9	
M_{23}	M_{11}	11	9	
${}^2F_4(2)'$	$2^2.\left[2^8\right]:S_3$	2^{11}	9	(1)
HS	M_{11}	11	9	
J_3	$L_2(16):2$	5	9	(2)
M_{24}	$2^6:(L_3(2)\times S_3)$	2^{10}	9	
M^cL	$U_4(3)$	3^6	9	
He	$S_4(4):2$	2^{10}	9	(3)
Ru	${}^2F_4(2)$	2^{14}	9	(4)
Suz	$2_{-}^{1+6}.U_4(2)$	2^{13}	9	
$O'N$	$L_3(7):2$	7^3	9	
Co_3	$2.S_6(2)$	2^{10}	9	
Co_2	$2_{+}^{1+8}:S_6(2)$	2^{18}	9	
Fi_{22}	$O_7(3)$	3^9	9	
HN	$2.HS.2$	11	27	(5)
Ly	$G_2(5)$	5^6	9	
Th	$2^5.L_5(2)$	2^{15}	9	
Fi_{23}	$S_8(2)$	2^{18}	9	(6)
Co_1	$2_{+}^{1+8}.O_8^{+}(2)$	2^{21}	9	
J_4	$2^{11}:M_{24}$	2^{21}	27	
Fi_{24}'	$3^7.O_7(3)$	3^{16}	9	
B	$2.{}^2E_6(2).2$	2^{41}	12	
M	$2.B$	2^{46}	36	

Table 1. Upper bounds on the minimal length of special solvable conjugate factorzations of simple sporadic groups and the Tits group

References

[1] M. Abért. Symmetric groups as products of abelian subgroups. *Bull. London Math. Soc.*, 34(4):451–456, 2002.

[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford (1985) (Reprinted with corrections 2003).

[3] L. Babai, N. Nikolov, and L. Pyber. Product growth and mixing in finite groups. In *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 248–257. ACM, New York, 2008.

[4] W. Bosma, J. Cannon and C. Playoust, "The Magma algebra system I, the user language", J. Symbolic Comput., 24(3-4):235–265, 1997.

[5] T. Breuer, CTblLib, - GAP's Character Table Library package, version 1.2.1, (2012), http://www.math.rwth-aachen.de/ ˜Thomas.Breuer/ctbllib

[6] T. Breuer and J. Müller, GAP file tst/mferctbl.gap, a compiled database of character tables of endomorphism rings of multplicity-free permutation modules of the sporadic simple groups and their cyclic and bicyclic extensions.

[7] T. Breuer, K. Lux, "The multiplicity-free permutation characters of the sporadic simple groups and their automorphism groups", Communications in Algebra, vol 24, number 7, (1996), 2293-2316

[8] J. Cannon, M. Garonzi, D. Levy, A. Maróti, and I. Simion. Groups equal to a product of three conjugates subgroups. 2014.

[9] R. W. Carter. Nilpotent self-normalizing subgroups of soluble groups. *Math. Z.*, 75:136–139, 1960/1961.

[10] R. W. Carter. *Finite groups of Lie type*. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication.

[11] R. W. Carter. *Simple groups of Lie type*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1989. Reprint of the 1972 original, A Wiley-Interscience Publication.

[12] V. Chernousov, E. W. Ellers, and Nikolai G. Gauss decomposition with prescribed semisimple part: short proof. *J. Algebra*, 229(1):314–332, 2000.

[13] K. Doerk and T. Hawkes. *Finite soluble groups*, volume 4 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1992.

[14] D. Easdown and C. E. Praeger. On minimal faithful permutation representations of finite groups. *Bull. Austral. Math. Soc.*, 38(2):207–220, 1988.

[15] H. Kurzweil and B. Stellmacher, The Theory of Finite Groups An Introduction, Springer (2004).

[16] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.5; 2013. (http://www.gap-system.org)

[17] M. Garonzi and D. Levy. Factorizing a finite group into conjugates of a subgroup. *J. Algebra*, 418:129–141, 2014.

[18] M. Garonzi, D. Levy, A. Maróti, and I. Simion. Minimal length products of unipotent Sylow subgroups in finite simple groups of Lie type. arXiv:1501.05678v1, 2015.

[19] M. Garonzi, D. Levy, A. Maróti, and I. Simion. Work in progress.

[20] D. Gorenstein, R. Lyons, and R. Solomon. *The classification of the finite simple groups. Number 3. Part I. Chapter A*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1998. Almost simple K-groups.

[21] B. Huppert. *Endliche Gruppen*, volume 134 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1967.

[22] G. Kaplan and D. Levy. Products of subgroups which are subgroups. *Comm. Algebra*, 35(5):1517–1523, 2007.

[23] L. G. Kovács and C. E. Praeger. On minimal faithful permutation representations of finite groups. *Bull. Austral. Math. Soc.*, 62(2):311–317, 2000.

[24] M. W. Liebeck, C. E. Praeger, and J. Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. Ser. A*, 44(3):389–396, 1988.

[25] M. W. Liebeck and L. Pyber. Finite linear groups and bounded generation. *Duke Math. J.*, 107(1):159–171, 2001.

[26] G. Malle and D. M. Testerman. *Linear algebraic groups and finite groups of Lie type*, volume 133 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2011.

[27] L. Pyber and E. Szabó. Growth in linear groups. In *Thin groups and superstrong approximation*, volume 61 of *Math. Sci. Res. Inst. Publ.*, pages 253–268. Cambridge Univ. Press, Cambridge, 2014.

[28] J. S. Rose. *A course on group theory*. Cambridge University Press, 1978.

[29] A. Smolensky. Unitriangular factorization of twisted Chevalley groups. *Internat. J. Algebra Comput.*, 23(6):1497–1502, 2013.

[30] A. Smolensky. Products of Sylow subgroups in Suzuki and Ree groups. arXiv: 1501.05234v1,arXiv:1501.05234v2, 2015.

[31] A. Smolensky, B. Sury, and N. Vavilov. Gauss decomposition for Chevalley groups, revisited. *Int. J. Group Theory*, 1(1):3–16, 2012.

[32] O. I. Tavgen′. Bounded generability of Chevalley groups over rings of S-integer algebraic numbers. *Izv. Akad. Nauk SSSR Ser. Mat.*, 54(1):97–122, 221–222, 1990.

[33] O. I. Tavgen′. Bounded generability of Chevalley groups over rings of S-integer algebraic numbers.Proceedings of the International Conference on Algebra Dedicated to the Memory of A. I. Mal'cev, Part 1, vol. CONM/131.1, Contemp. Math, 1992, pp. 409–421.

[34] N. A. Vavilov, A. V. Smolenskiĭ, and B. Sury. Unitriangular factorizations of Chevalley groups. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 388(Voprosy Teorii Predstavlenii Algebr i Grupp. 21):17–47, 309–310, 2011.

(Martino Garonzi) Departamento de Matematica, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Brasília - DF 70910-900, Brasil

E-mail address: `mgaronzi@gmail.com`

(Dan Levy) The School of Computer Sciences, The Academic College of Tel-Aviv-Yaffo, 2 Rabenu Yeruham St., Tel-Aviv 61083, Israel

E-mail address: `danlevy@mta.ac.il`

(Attila Maróti) Fachbereich Mathematik, Technische Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany, and Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

E-mail address: `maroti@mathematik.uni-kl.de` and `maroti.attila@renyi.mta.hu`

(Iulian I. Simion) Department of Mathematics, University of Padova, Via Trieste 63, 35121 Padova, Italy

E-mail address: `iulian.simion@math.unipd.it`